REMARKS

Reconsideration and allowance of the subject application in view of the foregoing amendments and the following remarks is respectfully requested. Entry of this Amendment Under Rule 116 is merited as it raises no new issues and requires no further search.

Claims 1-10, 12-32, and 35-43 remain pending.

The Examiner's withdrawal of the objection to claim 35 is noted with appreciation.

The Examiner's request for a substitute specification is not understood as only a single paragraph amendment inadvertently failed to indicate the text to be amended. A quick review of the text of the paragraph shows that a reference numeral, i.e., "78", was deleted from the first line of the paragraph. The amendment of the sixth paragraph beginning on page 17 is submitted again along with the previously submitted specification amendments as indicated above. A substitute specification is not believed necessary at this time as neither the number or nature of the amendments nor the legibility of the application papers renders it difficult to consider the application, or to arrange the papers for printing or copying.

Further, the Examiner incorrectly refers to the previously submitted amendments as failing to conform to 37 C.F.R. 1.125 (b) and (c); however, Applicant had not submitted a substitute specification under §1.125. Instead, Applicant submitted amendments to the specification under 37 C.F.R. 1.121 (b).

In view of the foregoing, the Examiner is requested to enter the submitted amendments and withdraw the requirement for submission of a substitute specification.

With respect to the Examiner's Response to Applicant's Arguments, Applicant disagrees with the Examiner's characterization of Moran (U.S. Patent 6,647,400) as anticipating claim 1 as Moran fails to disclose reformatting read kernel records into a different format, wherein the different format is a memory mapped file and parsing and comparing the kernel records against a template. There are at least three reasons the Examiner is in error.

First, column 11, lines 15-54 of Moran, discloses, at most, that the system is able to read "dump format" files, but fails to disclose reformatting read kernel records into a different format.

See specifically, column 11, lines 33-34, "Filesystem information . . . may be recovered from backup dumps." (emphasis added) In the absence of disclosure in Moran of reformatting read kernel records into a different format, the rejection should be withdrawn.

Second, column 27, lines 37-39 and column 29, lines 4-52 of Moran, fail to disclose the different format for records is a memory mapped file. Column 27, lines 37-39, disclose that a directory in a file system is a file which maps a file name to an i-node and column 29, lines 4-52, disclose a procedure for finding names of deleted files. Neither of the identified disclosures of Moran disclose a format for reformatted kernel records is a memory mapped file. For at least this reason, the rejection should be withdrawn.

Third, column 18, lines 6-58 of Moran, fail to disclose parsing and comparing the kernel records against a template. Instead, the identified portion of Moran describes the format for message transfers between sensors of the system and the analysis engine. According to Moran, sensor data may be transferred to the analysis engine using the described message header. This is not the same as parsing and comparing kernel records against a template.

Further, Moran at column 32, lines 44-58 discloses cross checking files with signatures of current versions of the file in a database. Moran fails to disclose comparing kernel records against a template according to the description of a template at page 28, lines 20-27 of the instant specification. Further still, a file signature is not the same as a template. That is, a file signature cannot be used as a representation of an algorithm to detect a vulnerability exploitation. For either of these reasons, the rejection should be withdrawn.

For each of the above reasons, claim 1 is patentable over Moran and the rejection should be withdrawn.

With respect to claim 29, column 32, line 44 - column 33, line 62 of Moran discloses checking files in system directories with file signatures in a package management database. Moran states that "most of the files of interest are not specific to an individual host, the need for precomputing signatures is largely eliminated." Moran at column 33, lines 49-51. That is,

Moran points out that most files to be compared are not tied to a particular host and file signatures from software distributions may be used for comparison instead of computing signatures for the particular host's files in advance. Moran fails to disclose the limitation of claim 29 that if a directory is specifically excluded and a file in the specifically excluded directory is specifically included the file is monitored. Moran fails to disclose a specifically included file in a specifically excluded directory and thus cannot disclose monitoring the specifically included file. For at least this reason, the rejection of claim 29 should be withdrawn.

Further, the Examiner has failed to address Applicant's remarks regarding claim 9 in view of Moran. That is, Moran fails to disclose the claim 9 limitation of encrypting information sent between the intrusion detection system and a network as at column 16, lines 15-29, Moran describes the passing of values between components of the system by performing data type conversions. Thus, Moran fails to disclose encrypting information transmitted. For at least this reason and the reasons advanced above with respect to claim 1 from which claim 9 depends, the rejection of claim 9 should be withdrawn.

Claims 2-10 and 12-28 depend, either directly or indirectly, from claim 1, include further important limitations, and are patentable over Moran for at least the reasons advanced above with respect to claim 1 and the rejection should be withdrawn.

Claims 30-32 and 35-43 depend, either directly or indirectly, from claim 29, include further important limitations, and are patentable over Moran for at least the reasons advanced above with respect to claim 29 and the rejection should be withdrawn.

All objections and rejections having been addressed, it is respectfully submitted that the present application should be in condition for allowance and a Notice to that effect is earnestly solicited.

Early issuance of a Notice of Allowance is courteously solicited.

The Examiner is invited to telephone the undersigned, Applicant's attorney of record, to facilitate advancement of the present application.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 08-2025 and please credit any excess fees to such deposit account.

Respectfully submitted,

LOWE HAUPTMAN & BERNER, LLP

Randy A. Noranbrock
Registration No. 42,940

1700 Diagonal Road, Suite 300
Alexandria, VA 22314
(703) 684-1111
(703) 518-5499 Facsimile
Date: June 13, 2005
KMB/RAN/iyr